Information Security Managers Group
Thursday, June 24, 2010 Meeting Minutes

MEETING LOGISTICS (all meeting minutes are posted on the ISMG Sharepoint site: http://ent.sharepoint.mt.gov/groups/ism/default.aspx)

When: Last Thursday of each month 1:00 pm – 2:30 pm
Who: Agency CIO and/or Information Security Manager
Where: Department of Labor and Industry First Floor Conference Room
Corner of Lockey and Sanders
Next Meeting: Tentative – August 26, 2010 1:00 pm

PRESENT

MDT:	Kristi Antosh
DLI:	Judy Kelly
DOC:	Larry Krause
DOA:	Kevin Winegardner - Chair
OPI:	Joan Anderson
HHS:	Jacklynn Thiel
HHS:	Chris Silvonen
MSL:	Jennie Stapp
DOR:	Di Wenger for Cleo Anderson

PURPOSE

The Information Security Managers Group has three primary purposes:

- Advise the State CIO on Information Risk Management Issues at the Statewide level
- Raise awareness while identifying communities of interest for EPP purposes
- Provide a forum for agency exchange of information

AGENDA ITEMS

- **Welcome and (re)introductions**
  - The Group members introduced themselves around the table.

- **Training on NIST Controls – Control Family – Program Management Control PM-2 = Senior Information Security Officer**
  - Discussion:
    - Group discussed NIST Control Family "Program Management", Conrtol PM-2, Senior Information Security Officer.

- **Action Item: Adopt Key Elements of an Information Security Program** and **Sample Outline of Information Security Program Plan.**
  - Action:
    - Group decided to adopt key program elements according to NIST Program Management Controls family.
    - More work is needed to refine outline of sample Information Security Program Plan.

- **Discussion:**
  - ISMG decided to postpone identification of associated Tasks required to achieve Objectives pending refinement of Objectives for the Information Security Program plan.

- **Status Update: State CIO decision package legacy IT policy: Usernames and Passwords**
  - State CIO has approved decision package.

- **Action Item: Discuss and provide recommendation to Chair for State CIO decision package on legacy IT policies:** Logging On and Logging Off Computer Resources and Remote Access for Employees and Contractors.
  - Review: The team applied previously determined criteria for a Statewide Information Security Policy, to the legacy IT policies under discussion to determine if they meet the criteria:
    - Statewide IT Security Policies must comply with State Statutes.
      - Determination: Pass.
    - Statewide IT Security Policies must be broadly applicable to all covered entities.
      - Determination: Fail.
        - The Policies are overly prescriptive.
    - Statewide IT Security Policies must align and address NIST Control Families at a Strategic level
      - Determination: Fail.
        - The Policies address only some parts of controls addressed by the NIST Access Control Family.
  - Recommendation of Development Team:
    - Of the three courses of action the development team was tasked to select from in reviewing the legacy IT policies:
      - Retain as written
      - Revise to align with NIST
      - Rescind the legacy IT policy
    - Based on the determination that the Policies fail to meet all minimum criteria to qualify as a Statewide IT Security Policies the team decided to recommend:
      - A single Statewide Standard that addresses the NIST Control Family "Access Control" be developed and published by the State CIO Policy Office. The legacy IT policies: "Logging On and Logging Off Computer Resources and Remote Access for Employees and Contractors", will be rescinded upon the effective date of the Statewide Standard: "Access Control", which will supersede it.
      - Additionally, the team decided to request that the State CIO Policy Office produce a "Statewide Guideline: Access Control" instrument, based on the NIST controls, as a companion instrument for the Standard.
  - Action Item to Chair:
    - Craft and deliver decision package to the State CIO containing the above recommendations.
    - Report status of decision package to ISMG at August 26 meeting.

- **ISMG reviewed and discussed** possible training opportunity by having MISTI bringing, 'Applying the NIST Information Risk Management Framework' and 'Managing an Information Security Program' seminars to the state. See complete list of seminars here: http://www.misti.com/default.asp?Page=31&Type=3&Cat=168
  - Action Item: All, please get a head-count of those individuals you would want to attend such training (target audience is ISM and ISSO's). E-mail head-count to Kristi Antosh kantosh@mt.gov or Kevin Winegardner kwinegardner@mt.gov .

- **Discussion regarding GSA RFP artifacts – Sample System and Service Acquisition controls.** See artifacts here: http://ent.sharepoint.mt.gov/groups/ism/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fgroups%2fism%2fShared%20Documents%2fSample%20System%20and%20Services%20Acquisition%20Artifacts&FolderCTID=&View=%7b1230E6FB%2d5351%2d475D%2dB022%2d749C1AC1FCA9%7d

FUTURE ITEMS

- Next NIST Control to review, Program Management control: PM-3 "Information Security Resources" Integrating the Information Security Program resource requirements into the Capital Planning and Investment Control process.

ACTION ITEMS

- Post adopted key elements of an Information Security Program, as promulgated in the NIST control family Program Management Controls.
    - ISMG Chair

- Refine the Objective's in the sample Information Security Program plan and post for discussion on the ISMG site.
    - ISMG Chair

- Post sample Statewide Standard: Identification and Authentication to the ISMG site for review to be discussed at next meeting.
    - ISMG Chair

- Craft Decision Package for the State CIO, recommending creation of; "Statewide Standard: Access Control" and "Statewide Guideline: Access Control".
    - ISMG Chair

- Review remaining legacy IT policies for action on disposition. E-mail ISMG Chair by 08/01/2010 with recommendations for next policy(ies) to review. Is there another group that belongs under an individual NIST Control family? List is here: http://ent.sharepoint.mt.gov/groups/ism/irmp/Legacy%20Policies/Forms/AllItems.aspx
    - Policy Development Team (ISMG)

- Develop a visual representation of Policy, Standard of Performance, Guideline, and Procedure taxonomy. Post to ISMG Sharepoint site. (Companion Visual to go with spreadsheet "Connect Dots Ext Req to Procedures" here: http://ent.sharepoint.mt.gov/groups/ism/ate/Policy%20Standard%20Guidelines%20Procedures%20Taxonomy/Forms/AllItems.aspx
    - ISMG Chair
- Develop a visual representation of Sample Program Implementation Strategy. Post to ISMG Sharepoint site. (Companion Visual to go with "Sample Program Implementation Strategy" document here: http://ent.sharepoint.mt.gov/groups/ism/irmp/Planning/Forms/AllItems.aspx?RootFolder=%2fgroups%2fism%2firmp%2fPlanning%2fNear%2dTerm&FolderCTID=&View=%7b9FBC1CC6%2dA447%2d4B8F%2d8F78%2d2B1E6E645E87%7d)
    - ISMG Chair

AGENDA ITEMS FOR NEXT MEETING

- Training on NIST Controls – Control Family – Program Management
    - Control PM-3 - "Information Security Resources". – ISMG Chair
- Review and discuss refined Objective's in the sample Information Security Program plan.
    - ISMG
- Report on Status: Decision Package for the State CIO, recommending creation of; "Statewide Standard: Access Control" and "Statewide Guideline: Access Control"
    - ISMG Chair
- Discuss and Determine recommendation on next legacy IT policies under review*: To be determined.
    - Development Team (ISMG)
- Review and discuss: sample "Statewide Standard: Identification and Authentication" for requirements determination.
    - ISMG